

Sections 103(a)(2) and (3) also require reliability with respect to LAES.¹⁰² If a carrier has not implemented measures to assess and confirm the reliability of a packet data intercept and its delivery to law enforcement, the carrier will have no way to assure law enforcement that it has reliably isolated, and reliably provided law enforcement with access to, CII and/or communications content.¹⁰³ Without such assurances, law enforcement will not be able to rely on the intercepted information. Moreover, given the delivery requirement in Section 103(a)(3), intercepted information that is not reliably delivered to law enforcement cannot be considered to be truly “delivered.”

B. The Commission Should Make Clear That Carriers Are Required to Provide Capabilities That Adequately Address Security, Performance, and Reliability

As discussed above, CALEA Section 103 requires carriers to implement capabilities that address security, performance, and reliability with respect to LAES. Indeed, industry has acknowledged this very requirement by including such capabilities in J-STD-025-B. But while J-STD-025-B includes security, performance, and reliability capability provisions, it merely imports the same limited provisions contained in J-STD-025-A, without taking into account the nature of the services to which J-STD-025-B is intended to apply.

Put simply, J-STD-025-B’s security, performance, and reliability provisions are

¹⁰² 47 U.S.C. § 1002(a)(2)-(3).

insufficient because they address the capability requirements from a circuit-mode – rather than a packet-mode – perspective and, therefore, will not ensure the security, performance, and reliability of packet data service intercepts. It is important to differentiate between the circuit-mode services that fall within the scope of J-STD-025-A and the packet-mode services that fall within the scope of J-STD-025-B. For circuit-switched services, the loss of some small amount of an intercepted communication, e.g., a millisecond of communications time, is imperceptible to the user as well as to law enforcement. For packet-based services, however, the loss of one or more packets may render the collection of an entire communication worthless if the packets lost are vital to the reconstruction of the communication. In other words, the nature of packet-mode services raises the bar for both the carrier and law enforcement. Completeness and reliability are critical; thus, reliance on the limited and vague provisions in J-STD-025-A to ensure the security, performance, and reliability of packet-based services is not adequate to meet the requirements and obligations in CALEA Section 103.

To be deemed to have met the requirements of Section 103, a standard must, at a minimum, include security, performance, and reliability capabilities for electronic surveillance that are at least equivalent to those used to determine and ensure the security, performance, and reliability of the carrier's network. Accordingly, DOJ requests that the Commission establish rules requiring carriers to (1) provide capabilities that address security, performance, and reliability with respect to LAES,

¹⁰³ *Id.* § 1002(a)(1)-(2).

and (2) take into account the adequacy of such security, performance, and reliability capabilities with respect to the service involved.

1. Security

J-STD-025-B is deficient because it fails to include security-related provisions that would, in the context of packet data services, ensure that LAES is undetectable to the subject and protect the fact of and access to an interception and information related thereto. Among the specific security capabilities that should be – but are not – included in J-STD-025-B are:

- The capability to ensure that LAES is unobtrusive – i.e., transparent to and not detectable by the intercept subject, the associates, and other parties to the communication;
- The capability to prevent unauthorized communications and CII from being intercepted;
- The capability to protect the assistance capabilities used to facilitate LAES;
- Capabilities to protect the confidentiality of LAES activities (e.g., preventing knowledge of the fact that LAES is being conducted; technical security mechanisms for activating/deactivating LAES or accessing captured CII or communications content; preventing LAES subjects from being notified of service changes caused by LAES);
- The capability to protect information regarding the government's interception of communications and access to CII; and
- The capability to protect (securely deliver) the packet data streams as they are delivered to law enforcement.¹⁰⁴

¹⁰⁴ CALEA Section 103(a) requires this insofar as it provides that carriers must “facilitat[e] authorized communications interceptions and access to call-identifying information unobtrusively” and “in a manner that protects . . . the government’s interception of communications and *access to call-identifying information.*” 47 U.S.C.

The security capability requirements in Section 103 can only be satisfied by requiring security-related capabilities, with quantitative measures that assess and ensure the overall security of a given interception. J-STD-025-B's lack of adequate security-related capabilities not only fails to meet Section 103's security requirements, but threatens to compromise law enforcement's investigations. For example, a subject could become aware of an interception or be inadvertently notified of a change in service, or an unauthorized interception of communications content or CII could be conducted.

Thus, a carrier that fails to deploy capabilities that adequately address the security requirements in Section 103 – or relies on a standard that does not adequately address the security requirements in Section 103 in the context of the services to which that standard is intended to apply – cannot be deemed to have complied with its statutory obligations under CALEA. Accordingly, DOJ requests that the Commission require carriers to provide security-related capabilities that address the requirements of Section 103 in the context of the service(s) involved.

2. Performance and Reliability

As discussed above, CALEA Sections 103(a)(2) and (3) require carriers to isolate and deliver intercepted communications content and CII to law enforcement.¹⁰⁵ Complete, accurate, and reliable collection and delivery of the intercepted information

§ 1002(a)(4) (emphasis added).

¹⁰⁵ 47 U.S.C. § 1002(a)(2)-(3).

is implicit in this requirement. CALEA requires that carriers isolate and enable the government to intercept "*all* wire and electronic communications carried by the carrier. . . to or from equipment, facilities, or services of a subscriber"¹⁰⁶ and deliver such intercepted communications to the government.¹⁰⁷ As noted previously, this is particularly true in the case of packet data services, where even tiny inaccuracies in delivery can render a communication unusable by law enforcement. These provisions necessarily require that carriers use quantitative performance and reliability measures to assess and confirm the completeness and reliability of both the interception *and* the delivery of the intercepted communications to law enforcement.¹⁰⁸

Notwithstanding these requirements, J-STD-025-B does not contain any quantitative performance and reliability measures, such as packet loss or bit error rate, which are designed to assess and ensure the completeness and reliability of intercepts. For example, J-STD-025-B fails to include any measures that address packet loss of communications content after an interception (i.e., the loss or omission of packets from the communications stream). Lost or omitted packets present significant technical problems in reassembling packet data communications. Effectively and accurately

¹⁰⁶ 47 U.S.C. § 1002(a)(1) (emphasis added).

¹⁰⁷ *Id.* § 1002(a)(3).

¹⁰⁸ With respect to delivery, if the completeness and reliability of the intercepted information being delivered to law enforcement cannot be confirmed by the carrier, the carrier cannot be said to have actually "delivered" the intercepted communications content and CII to law enforcement as required by Section 103(a)(3).

reassembling a subject's broadband communication stream into the associated individual applications (e.g., web browsing, e-mail, instant messaging) requires access to the subject's complete packet stream; the loss, omission, or corruption of key packets within the subject's communication stream during transmission from the carrier makes it difficult, if not impossible, for law enforcement to reassemble the associated application-level communications.¹⁰⁹ This loss would severely damage law enforcement's ability to conduct LAES. Without performance and reliability measures in place to help it determine whether or not a packet has been lost, dropped, or corrupted, law enforcement will not be able to ensure that it has received all of the intercepted communications and CII to which it is legally entitled.¹¹⁰

¹⁰⁹ DOJ is not requesting that carriers be responsible for any application level processing, but rather that the delivery solution to law enforcement ensure that packet loss is avoided so that law enforcement can successfully perform such processing.

¹¹⁰ Two cost-effective performance and reliability methods that would solve this problem are near-real-time delivery of communications content to a law enforcement co-located collection device, or carrier-provided buffering and retrieval of LAES over a secure VPN. DOJ urges the Commission to direct that the performance and reliability deficiencies in the standard be addressed via one of these methods. Mandating that law enforcement agencies procure a dedicated, high-bandwidth facility from the carrier to law enforcement would be neither a cost-effective nor a time-efficient solution to the problem. For example, VPNs can be set up within hours, while dedicated high-bandwidth facilities take a substantial amount of time to install (typically 30 days or more). The timeliness and completeness of delivery of lawfully authorized target communications to law enforcement is not only required by CALEA, but is also critical to law enforcement's ability to accomplish its mission. Delays in the delivery of lawfully authorized target communications to law enforcement could render the communications unusable by law enforcement, and would amount to a waste of time and resources for all concerned. DOJ notes, however, that to the extent a buffering solution is utilized, carriers may need to examine the impact of this solution on the

Quantitative performance and reliability measures such as packet loss and bit error rate are routinely used by carriers to assess and confirm the Completeness, quality, and reliability of communications transmitted on and over their networks. Because law enforcement has a similar need to confirm the completeness, quality, and reliability of the information provided to it, the Commission should require carriers to use these measures for purposes of satisfying the requirements of Section 103. Such measures will help to assure law enforcement that the CII and communications content has been collected by the carrier and delivered to law enforcement in a reliable, secure, and error-free manner that protects the integrity of the intercepted communications. Moreover, Sections 103(a)(2) and (3) necessarily require the use of such measures because omissions and errors cannot be identified and addressed without them.

As a general principle, the measures used by a carrier to assess the quality of the transmission of CII and communications content to law enforcement pursuant to CALEA Section 103 should be comparable – if not equivalent to – those it uses to measure the quality of transmissions on/over its own network. The reliability of the LAES intercept should likewise be at least equal to the highest level of reliability for the carrier’s underlying service.”” Satisfaction of the performance and reliability capability requirements in Section 103 can be assured only by requiring carriers to implement

timing capability (i.e., delivery of intercepted communications to law enforcement within 8 seconds).

¹¹¹ Typically, carriers’ service level agreements dictate the level of reliability offered to a customer.

adequate performance and reliability-related capabilities in connection with LAES. Moreover, without such capabilities, law enforcement investigations may be significantly compromised.

Thus, a carrier that fails to provide capabilities that address the performance and reliability requirements in Section 103 – or relies on a standard that does not adequately address the performance and reliability requirements in Section 103 in the context of the services to which that standard is intended to apply – cannot be deemed to have complied with its statutory obligations under CALEA. Accordingly, DOJ requests that the Commission require carriers to provide performance- and reliability-related capabilities that address the requirements of Section 103 in the context of the services involved

VI. The Commission Should Establish Rules Requiring Carriers to Provide the Additional and Modified Capabilities Identified in This Petition in Order To Meet the Assistance Capability Requirements of CALEA

CALEA Section 107(b) provides that if a standard-setting organization's "requirements or standards are deficient," the Commission "may establish, by rule, technical requirements or standards" that:

- (1) meet the assistance capability requirements of Section 103 by cost-effective methods;
- (2) protect the privacy and security of communications not authorized to be intercepted;
- (3) minimize the cost of such compliance on residential ratepayers;
- (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- (5) provide a reasonable time and conditions for compliance with and the transition to any new standard,

including defining the obligations of telecommunications carriers under section 103 during any transition period.¹¹²

The requested capabilities are necessary to meet CALEA's assistance requirements, which are in turn vital to protecting public safety and national security.¹¹³ Accordingly, for the reasons described below, the adoption of Commission rules requiring the additional and modified capabilities described in this Petition is warranted under CALEA Section 107(b).

A, Adopting the Capabilities Identified in this Petition Will Meet the Assistance Capability Requirements of CALEA Section 103 by Cost-Effective Methods

Although CALEA does not define the term "cost effective,"¹¹⁴ the Commission established in its *Order on Remand* a process by which to evaluate whether a given capability is "cost-effective":

[W]e first inquire whether we have in the record an alternative means to accomplish each of the punch list capabilities. . . . If we cannot make a cost comparison, we will consider other ways of determining whether a punch list capability is "cost-effective." . . . In general, something is "effective" if it accomplishes a task in an efficient manner.¹¹⁵

The Commission further noted in the *Order on Remand* that it would not "adopt or reject a capability solely on the basis of a cost-benefit analysis because Congress already has

¹¹² 47 U.S.C. § 1006(b).

¹¹³ *Id.* § 1002.

¹¹⁴ *Order on Remand* at 6914 ¶ 57.

¹¹⁵ *Id.* at 6914-16 ¶¶ 57-58.

made such a calculation when it determined the assistance capability requirements of CALEA.”¹¹⁶

No reasonable alternatives for providing these capabilities to law enforcement were presented by the TIA membership during J-STD-025-B's development. But even if alternative proposals are advanced by industry with respect to providing the additional and modified capabilities, the Commission should nonetheless – consistent with its previously established evaluation process – consider simply whether these capabilities provide law enforcement with required CII in an efficient manner.

Commercial "off-the-shelf" hardware and software is already readily available that could be adapted to enable carriers to provide the CII-related capabilities requested in this Petition. In fact, numerous companies (e.g., trusted third party service bureaus, CALEA solution vendors, equipment manufacturers) have emerged over the past several years that specialize in providing telecommunications carriers with CALEA solutions for their packet-mode services. As a result, CALEA solutions often are now much less costly and burdensome to install than in the past. Thus, satisfying the requirements of CALEA by providing the capabilities requested in this Petition can be accomplished efficiently and by cost-effective methods.

¹¹⁶ *Id.* at 6916 ¶ 58. Noting that there are costs associated with CALEA that Congress clearly anticipated carriers would bear, the Commission refused to "reject the punch list capabilities solely because they would be costly to implement. . . ." *Id.* at 6916 ¶ 59.

B. The Capabilities Identified in This Petition Will Help Protect the Privacy and Security of Communications

Each of the requested capabilities will help protect the privacy and security of communications not authorized to be intercepted.

1. Packet Activity Reporting

Packet activity reporting CII enables law enforcement to identify the parties involved in a communication and the types of services used by the subject. In the absence of a packet activity reporting capability, carriers have no means by which to isolate certain CII from other information, including communications content, and deliver only the isolated CII to law enforcement.¹¹⁷ As a result, law enforcement will have no other practical alternative than to attempt to do the separation itself in order to ensure compliance with court orders and other authorizations. This situation is exactly the kind that CALEA sought to avoid. Thus, as more fully discussed above,¹¹⁸ requiring a packet activity reporting capability helps protect the privacy and security of communications by harmonizing CALEA's goal of protecting the privacy of communications not authorized to be intercepted with the government's authority to collect CII.¹¹⁹

¹¹⁷ 47 U.S.C. § 1002(a)(1)-(2).

¹¹⁸ See *supra* Section IV.A.

¹¹⁹ See 47 U.S.C. §§ 1002(a)(2), (a)(4)(A), 1006(b)(2).

2. Timing Information (Time Stamping)

The Commission already has concluded, without raising any privacy concerns, that a timing information (time stamping) capability is necessary to implement CALEA.¹²⁰ Likewise, there are no privacy concerns with requiring a timing information (time stamping) capability for CDMA2000 data services.

3. Location Information

The location information capability also does not impact any legitimate privacy interest because it would not provide any information that law enforcement is not authorized to receive. CALEA directs the Commission to adopt rules that "protect the privacy and security of communications *not authorized to be intercepted*"¹²¹ DOJ asks the Commission to require that carriers deliver to law enforcement all signaling that reveals mobile handset location information only when (1) law enforcement has obtained the appropriate legal authorization to receive such information, and (2) such information is "reasonably available" to the carrier. DOJ's request satisfies CALEA Section 107(b)(2)'s privacy prong because the requested capability would not allow law enforcement to access any information that it is not lawfully authorized to receive. To the extent the Commission chooses to evaluate the privacy impact of the location

¹²⁰ See *Third R&O* at 16835-36 ¶¶ 95-96.

¹²¹ 47 U.S.C. § 1006(b)(2) (emphasis added).

capability requested in this Petition,¹²² however, the conclusion that the requested capability would not unduly intrude on any privacy interest remains the same.

When it crafted Section 103(a)(2), Congress considered the effect on privacy of enabling law enforcement to access location information. In that Section, Congress specified one situation in which location information *cannot* be provided to law enforcement: when law enforcement has only a pen register or trap and trace order.¹²³ This is a unique provision in a statute that otherwise does not address legal authority at all. By foreclosing only one means for obtaining access to location information, Congress implicitly expressed an expectation that other legal authorities *could* authorize law enforcement to obtain a subscriber's mobile handset location information. In addition, both the Commission and the D.C. Circuit have confirmed that location information is CII under CALEA.¹²⁴

As discussed above, DOJ's request for access to signaling that reveals mobile handset location information is consistent with CALEA and with the Commission's prior approach to location information capabilities. First, regardless of a requirement to provide law enforcement with more precise location information when it is reasonably available to the carrier, law enforcement still must have appropriate legal authorization

¹²² Should the Commission decide to conduct a privacy analysis of this capability, the Commission should describe the factors it will use in reaching its conclusion.

¹²³ 47 U.S.C. § 1002(a)(2)(B)

¹²⁴ *Third R&O* at 16815 ¶ 44; *United States Telecom. Ass'n*, 227 F.3d at 463-64.

before it may access any such information. Second, law enforcement still will be able to access such mobile handset location information only at the beginning and the end of each communication. The only difference between the capability requested in this Petition and that adopted in the *Third R&O* and currently provided in J-STD-025-B is that the former would provide law enforcement with a *more* accurate and precise version of the location information at the beginning and the end of a communication (i.e., latitude/longitude information, versus a mobile cell site identifier). Accordingly, the distinction is not the identification of the location of a mobile handset *per se*, but the *more accurate and precise* identification of that mobile handset's location.

Wireless subscribers' privacy will be protected even if carriers provide law enforcement with more accurate location-based CII, since a location information capability is already included in J-STD-025-B. But even assuming *arguendo* that the more precise location information capability raises more significant privacy concerns than the existing capability, the inclusion of the requested toggle feature – with a default setting of "off" – will reasonably ensure the privacy of information not authorized to be intercepted by ensuring that carriers provide to law enforcement only the information authorized to be accessed.

4. Security, Performance and Reliability Capabilities

The modified security capabilities that DOJ seeks will "protect the security and privacy of communications not authorized to be intercepted."¹²⁵ As described above, the requested capabilities include controls that ensure that LAES is undetectable to the subject, and that protect the fact of, and access to, an interception and information related thereto. Moreover, these capabilities safeguard the equipment and mechanisms used to perform intercepts, and protect the packet data streams as they are delivered to law enforcement.¹²⁶ Indeed, the very purpose of such capabilities is to protect the security and privacy of communications not authorized to be intercepted. Accordingly, the security capabilities sought would advance CALEA's goal of protecting the security and privacy of such communications.

C. The Additional and Modified Capabilities Minimize the Cost of Compliance on Residential Ratepayers

The additional and modified capabilities requested by DOJ can be implemented cost-effectively and in a manner that minimizes the costs of compliance on residential ratepayers, as many of the capabilities described already exist in carriers' networks, or

¹²⁵ 47 U.S.C. § 1006(b)(2). The modified performance and reliability capabilities sought by DOJ have no impact on the security or privacy of communications *per se*, as they are designed to ensure that the intercepted communications are actually and accurately delivered to law enforcement. To the extent that these performance and reliability capabilities ensure that intercepts are performed in accordance with the legal authorization, then these capabilities also protect the security and privacy of communications from inadvertent or mistaken collection.

¹²⁶ See Section V *supra*.

can be implemented with relatively minimal cost.

Many of the capabilities described in this Petition exist in carriers' networks and have already been paid for by the affected carriers. For example, wireless carriers have paid for the E-911 Phase II location information capability that has been deployed in their networks.¹²⁷ Providing this same capability for CALEA purposes should add very little, if any, to carriers' E-911 Phase II development costs, and should therefore minimize the cost of compliance on residential ratepayers. The cost of providing a timing information (time stamping) capability to law enforcement also would be minimal, at most, because the same capability already is present and available in the affected carriers' networks. Similarly, because performance and reliability measures (e.g., packet loss, bit error rate) are currently present in, and routinely used by carriers to assess the completeness, quality, and accuracy of communications transmitted on their networks, there should be little or no additional costs associated with providing these capabilities for purposes of CALEA.

Moreover, the cost of implementing the requested capabilities in a packet-based network is likely to be significantly less than in traditional circuit-switched networks, because large switches need not be replaced and many third party providers offer these

¹²⁷ Some carriers chose to incur these costs themselves while others included a small monthly customer surcharge passed through on customer bills to recover the costs of such upgrades.

capabilities to industry at competitive prices.¹²⁸

Finally, even assuming the carrier must incur some costs to provide such capabilities, just as with the additional capabilities that were adopted by the Commission in the original J-STD-025 proceeding and later added to the standard, the cost of carrier compliance should have minimal impact on residential ratepayers. As the Commission recognized in the *Order on Remand*:

[I]t is likely that the cost would be shared by all ratepayers and, therefore, would be significantly diluted on an individual residential ratepayer basis. The fact that costs are spread across such a large base in itself suggests another means by which provision of these capabilities will minimize the effect on residential ratepayers – that the cost of CALEA compliance for any particular ratepayer will be

¹²⁸

See In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 15011 n.127 (2005) ("*First R&O*") (finding that industry solutions appear to be readily available); *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Second Report and Order and Memorandum Opinion and Order, 21 FCC Rcd 5360, 5372 ¶ 26 (2006). Furthermore, many broadband carriers have utilized network monitoring capabilities, such as packet inspection and packet capture (PCAP), to identify unauthorized and inappropriate use of their network (e.g., SPAM; Denial of Service (DoS) attacks, etc.). (See <http://www.winvcav.org/> and <http://www.tcpdump.org/> for more information on PCAP). Capabilities such as Multiprotocol Label Switching (MPLS) give network operators a great deal of flexibility in implementing Quality of Service (QoS) capabilities and assuring reliable transport of communications within their networks. The wide-scale adoption of Network Time Protocol (NTP) in IP networks provides a means of accurately synchronizing the internal clocks of IP-based network equipment. (For more information, see Network Time Protocol (NTP), IETF RFC 958, Sept. 1985; NTP.ORG, Home of the Network Time Protocol Project, viewable at <http://www.ntp.org/>). All of these capabilities – which are already implemented in many carrier networks – could be leveraged in order to address the capabilities described in this Petition.

minimal.¹²⁹

Accordingly, DOJ believes the requested capabilities can be provided at a minimal incremental cost to carriers, resulting in little or no cost to residential ratepayers.

D. The Additional and Modified Capabilities Are Consistent With the Commission's Policy of Encouraging the Provision of New Technologies and Services to the Public

The additional and modified capabilities described in this Petition are consistent with CALEA Section 107(b)(4) in that they "encourage the provision of new technologies and services to the public."¹³⁰ DOJ does not seek to delay or stop the deployment of any service to which J-STD-025-B would apply. DOJ does not believe that requiring the requested capabilities would have that effect. Nor was any evidence presented during the J-STD-025-B development process that requiring the additional and modified capabilities discussed in this Petition would discourage the provision of packet-mode (data) services. In fact, over the past several years, the FBI has worked actively with vendors and their carrier clients in an effort to facilitate the development of complete packet-based CALEA solutions for the marketplace that could be deployed simultaneously with the launch of CDMA2000 technologies and services. Indeed, based on these efforts, DOJ understands that several vendors have developed new CALEA solutions intended for CDMA2000 packet data services that can be deployed in a

¹²⁹

Order on Remand at 6919-20 ¶ 65

carrier's network when service is launched.

E. Twelve Months Is a Reasonable Transition Period Within Which to Incorporate the Capabilities Described in this Petition

Consistent with its comments on the *CALEA NPRM*,¹³¹ DOJ believes that twelve months after the effective date of the Commission's decision in this proceeding is an appropriate compliance period.^{132,133} The carriers that will be affected by the Commission's decision in the instant deficiency petition proceeding are already covered by CALEA and have been aware of CALEA's packet data compliance obligations since August 1999.¹³⁴ Moreover, TIA and industry have been aware of the additional and

¹³⁰ 47 U.S.C. § 1006(b)(4).

¹³¹ *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, 19 FCC Rcd 15676(2004) ("CALEA NPRM").

¹³² DOJ Comments on *CALEA NPRM*, at 57 (filed Nov. 8, 2004); DOJ Reply Comments on *CALEA NPRM*, at 46-47 (filed Dec. 21, 2004). Although the Commission ultimately concluded in the CALEA rulemaking proceeding that eighteen months was a reasonable time period for CALEA compliance by newly covered entities, see *First R&O* at 14990 ¶ 3, that decision should not be controlling here, because the requirement in the *First R&O* is applicable to entities that are newly covered by CALEA. A compliance time period adopted with respect to the application of CALEA to a given group of carriers or other entities pursuant to CALEA Section 102 should not apply to a deficiency petition filed under Section 107(b).

¹³³ DOJ notes, however, that there are limited circumstances in which a twelve-month compliance period may not be appropriate. For example, where air-to-ground wireless or broadband Internet access services have been deployed on commercial aircraft, a twelve-month gap in compliance would be excessive given the risk that terrorists or other criminals might use such services to communicate before or after taking control of an aircraft.

¹³⁴ *Third R&O* at 16795 ¶ 1.

modified capabilities requested in this Petition since at least 2001, when the FBI raised them at the outset of the J-STD-025-B standard development process. Given the facts and circumstances involved, a twelve-month compliance schedule is both reasonable and appropriate.¹³⁵ In addition, based upon DOJ's significant prior experience in working with wireless carriers deploying packet data CALEA solutions, twelve months has proven to be an adequate amount of time for carriers and their vendors to deploy such packet data solutions.

In the *Order on Remand*, the Commission clearly recognized that separate and unique CALEA compliance periods under CALEA Section 107(b)(5) are appropriate.¹³⁶ There, the Commission required – based on the particular facts, circumstances, and record in that proceeding – that carriers deploy the additional punch list capabilities for

¹³⁵ The text in Section 107(b)(5) clearly shows that Congress expected the Commission to adopt a unique time frame for carrier compliance as part of the deficiency petition process on the basis of the particular facts and circumstances presented. See 47 U.S.C. § 1006(b)(5) (directing the Commission to provide a reasonable time and conditions for compliance). Otherwise, this language would have been superfluous. See *Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979) (“In construing a statute we are obliged to give effect, if possible, to every word Congress used”). Congress included Section 107(b)(5) in CALEA because it recognized that the Commission's evaluation of deficiency petitions challenging CALEA standards would differ based on the facts and circumstances involved. Because the carriers that will be affected by the Commission's decision in the instant deficiency petition proceeding are already covered by CALEA and have been aware of CALEA's packet data compliance obligations for quite some time, a shorter compliance period that takes these facts into account is reasonable and appropriate.

¹³⁶ *Order on Remand* at 6941-42 ¶ 127.

J-STD-025 within just two months.¹³⁷ The Commission's decision to adopt a relatively short compliance deadline was based on a number of factors, including (1) carriers' ability to typically put into effect any required changes to their network within six months of a Commission decision; (2) that much of the software required to implement the punch list items has already been developed, thereby significantly speeding implementation; and (3) carriers' significantly greater experience in meeting CALEA's capabilities than in the earlier stages of CALEA's implementation.¹³⁸ The Commission concluded that these factors – when taken together – made a shorter implementation timetable reasonable.¹³⁹

The Commission's approach in the *Order on Remand* clearly recognized that the compliance period for deploying capabilities resulting from a deficiency proceeding can and should differ, based on the facts, circumstances, and record in a particular deficiency proceeding. There appears to be no reason to depart from that approach here. The majority of the additional and modified capabilities will not require a significant amount of effort to implement. The timing information (time stamping) capability is already included in J-STD-025-A and provided by carriers. Therefore, incorporating this capability into J-STD-025-B with respect to packet data services will require only minimal effort. Implementing the more precise location information

¹³⁷ *Id.*

¹³⁸ *Id.*

capability into J-STD-025-B should also not require a significant amount of effort, because the information already exists in wireless carriers' networks as a result of the Commission's E-911 Phase II requirement and because the proposed capability already takes account that such information be "reasonably available" to the carrier. In addition, although developing more robust capabilities to address security, Performance, and reliability in the context of packet data services will require a certain amount of effort, that effort should be minimal. A twelve-month compliance period is warranted based on the facts and circumstances concerning J-STD-025-B and, therefore, the Commission should require telecommunications carriers to begin providing the additional and modified capabilities to law enforcement within twelve months after the effective date of the Commission's decision in this proceeding.

VII. Conclusion

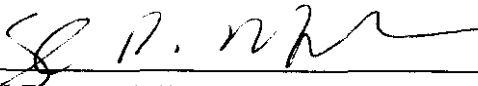
For all of the foregoing reasons, DOJ respectfully requests that the Commission find that J-STD-025-B is deficient with respect to meeting the assistance capability requirements of CALEA because it does not provide the following required capabilities: (1) packet activity reporting; (2) timing information (time stamping); (3) all reasonably available handset location information at the beginning and the end of a communication; and (4) adequate security, performance, and reliability requirements. DOJ further requests that the Commission establish rules requiring telecommunications carriers to provide the above-described additional and modified capabilities. Finally, DOJ requests that the Commission require telecommunications carriers to provide the

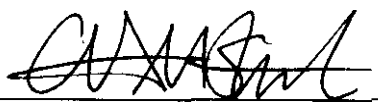
139 Id.


additional and modified capabilities within twelve months after the effective date of the Commission's decision in this proceeding.

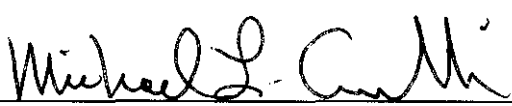
Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE


Sigal P. Mandelker
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530


Charles M. Steele
Chief of Staff
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530


Elaine N. Lammert
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
United States Department of Justice
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535


Michael L. Ciminelli
Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
United States Department of Justice
Washington, D.C. 20537

Dated: May 15, 2007

I, John R. Delmore, hereby certify that on this 15th day of May, 2007, I caused a true and correct copy of the **“Petition for Expedited Rulemaking,”** pertaining to “In the Matter of Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act” to be served upon the following parties as indicated:

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, **S.W.**
Washington, D.C. 20554

(via hand-delivery)

Derek Poarch, Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

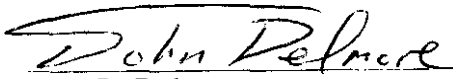
(via e-mail)

Dana Shaffer, Deputy Bureau Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington. D.C. 20554

(via e-mail)

Tom Beers, Deputy Chief
Policy Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington. D.C. 20554

(via e-mail)


John R. Delmore